Journal of Number Theory **93**, 23–33 (2002)
doi:10.1006/jnth.2001.2706, available online at http://www.idealibrary.com on IDEAL®

On Primitive Roots of One-Dimensional Tori[1]

Yen-Mei J. Chen

Department of Mathematics, Tamkang University, Tamshui, Taipei, Taiwan
E-mail: ymjchen@mail.tku.edu.tw

Communicated by D. Goss

Received June 10, 2000

We exploit an analogue of Artin's primitive roots conjecture for one-dimensional tori over $\mathbb{Q}$. Let $\mathbb{T}$ be a one-dimensional torus over $\mathbb{Q}$, and let $P \in \mathbb{T}(\mathbb{Q})$ be a nontorsion point. Under Generalized Riemann Hypothesis, we derive an explicit density formula for the set of rational primes ℓ such that P modulo ℓ generates

INTRODUCTION

Let $\mathbb{T}$ be a one-dimensional torus over $\mathbb{Q}$, and let $P = (x_0, y_0) \in \mathbb{T}(\mathbb{Q})$ be a nontorsion point. We are interested in the set M_P consisting of rational primes ℓ where $\mathbb{T}$ has good reduction $\tilde{\mathbb{T}}$ and P modulo ℓ generates the abelian group $\tilde{\mathbb{T}}(\mathbb{F}_\ell)$. The case $\mathbb{T} = \mathbb{G}_m$ dates back to Artin. The well-known Artin's conjecture (1927) asserts that for every nonzero non-square rational integer $a \neq \pm 1$ the set of rational primes ℓ for which a is a primitive root possesses a positive density. This conjecture was proved by Hooley [3] in 1967 under the Generalized Riemann Hypothesis (GRH). The purpose of this paper is to generalize Hooley's Theorem to all one-dimensional tori over $\mathbb{Q}$.

Our main result is the following.

THEOREM 1. *Let $\mathbb{T}$ be a one-dimensional torus over $\mathbb{Q}$, and let $P \in \mathbb{T}(\mathbb{Q})$ be a nontorsion point. Assume GRH holds. Then the set M_P has a (Dirichlet) density, given by* $\operatorname{den}(M_P) = \delta \cdot A$, *where* $A = \prod_{q \text{ prime}} (1 - \frac{1}{q(q-1)})$ *is the Artin's constant and δ is a rational number, which can be explicitly determined from $(\mathbb{T}, P)$. Moreover, we have $\delta > 0$ if and only if $P \notin \mathbb{T}(\mathbb{Q})^q$ for all primes q dividing $^{\#}Tor(\mathbb{T}(\mathbb{Q}))$.*

[1] Research partially supported by National Science Council, Republic of China.

0022-314X/02 $35.00

In view of Hooley's work, we only need to consider those tori $\mathbb{T}$ which are not isomorphic to $\mathbb{G}_m$ over $\mathbb{Q}$. However, any such torus is isomorphic to $\mathbb{G}_m$ over an unique quadratic field K, because the only automorphisms of $\mathbb{G}_m$ are $\pm\mathrm{id}$. Therefore, such torus $\mathbb{T}$ can be described by a quadratic equation of the form $x^2-my^2=1$, where m is a square-free integer. And there exists a bijective map Ψ from $\mathbb{T}(\mathbb{Q})$ to the set V_K of elements in $K=\mathbb{Q}(\sqrt{m})$ with norm 1: $\Psi\colon (x, y) \leftrightarrow x+y\sqrt{m}$. Denote the image of P under Ψ by α. i.e. $\alpha = x_0 + y_0\sqrt{m}$. Denote by M_α the set of rational primes ℓ where $K/\mathbb{Q}$ is unramified and α modulo ℓ has order $\ell-1$(resp. $\ell+1$), if ℓ splits (resp. is inert) in K. Then M_α and M_P only differ by a finite set and Theorem 1 is an immediate consequence of the following Theorem 2.

THEOREM 2. *Let K be a quadratic field and given $\alpha \in V_K$, which is not a root of unity. Assume GRH holds. Then* $\mathrm{den}(M_\alpha) = \delta \cdot A$, *where δ is a rational number explicitly determined from* (K, α).

Moreover, we have

$$\delta > 0 \Leftrightarrow \begin{cases} \alpha \notin (V_K)^2 & \text{if} \quad K \neq \mathbb{Q}(\sqrt{-3}), \\ \alpha \notin (V_K)^2 \cup (V_K)^3 & \text{if} \quad K = \mathbb{Q}(\sqrt{-3}). \end{cases}$$

In Section 1, we set up the notations and introduce some algebraic tools. In Section 2, we calculate the density assuming GRH. Theorem 2 is proved in Theorem 2.2 and Theorem 2.5. Finally we note that both Roskam [6] and Chen *et al.* [1] have proved a special case of Theorem 2, where K is taken to be real quadratic and α a fundamental unit.

1. ALGEBRAIC PRELIMINARIES

Let m be a fixed square-free integer, $K=\mathbb{Q}(\sqrt{m})$, and $\alpha = x_0 + y_0\sqrt{m}$ a fixed element in K with $N_{\mathbb{Q}}^K \alpha = 1$, which is not a root of unity. Let σ_0 denote the generator for the Galois group of K over $\mathbb{Q}$, and let τ denote the complex conjugation. Denote $\mathbb{P}$ to be the set of rational prime numbers, and $\mathbb{F}_r$ to be the finite field with r elements.

Notations. Let $q \in \mathbb{P}$.

$$E_1 = K, \qquad K' = \mathbb{Q}\left(\sqrt{\alpha}+\frac{1}{\sqrt{\alpha}}\right), \qquad K'' = \mathbb{Q}\left(\sqrt{\alpha}-\frac{1}{\sqrt{\alpha}}\right).$$

$\boldsymbol{\mu}_q =$ the group of qth roots of unity.

$E_q = K(\boldsymbol{\mu}_q, \sqrt[q]{\alpha})$.

$E_n = \prod_{q|n} E_q$ for any square free positive integer n.

$G_n =$ the Galois group of E_n over $\mathbb{Q}$.

$d_n = {}^{\#}G_n = [E_n : \mathbb{Q}]$.

$C_n^- = \{\sigma \in G_n : \sigma|_K = \sigma_0, \sigma|_{\mathbb{Q}(\mu_n)} = \tau, \sigma^2 = \mathrm{id}, \text{ and } \sigma|_{K'} = \mathrm{id} \text{ if } 2 \mid n\}$.

$c_n^- = {}^{\#}C_n^-$.

$(\ell, E/\mathbb{Q})$ is the Artin symbol, where $E/\mathbb{Q}$ is finite Galois and prime ℓ is unramified in E.

Remark. Suppose $\alpha \in (K^\star)^2$, i.e., $\sqrt{\alpha} \in K$. If $N_{\mathbb{Q}}^K \sqrt{\alpha} = 1$, then clearly $\mathrm{den}(M_\alpha) = 0$. Hence, we are interested only in the case that $N_{\mathbb{Q}}^K \sqrt{\alpha} = -1$, whenever $\alpha \in (K^\star)^2$. In this case, K has to be real, $K' = K$, and $K'' = \mathbb{Q}$.

PROPOSITION 1.1. (a) *If ℓ splits in K, then ${}^{\#}\tilde{\mathbb{T}}(\mathbb{F}_\ell)$ is cyclic of order $\ell - 1$.*

(b) *If ℓ is inert in K, then ${}^{\#}\tilde{\mathbb{T}}(\mathbb{F}_\ell)$ is cyclic of order $\ell + 1$.*

Proof. (a) If ℓ splits in K, then $\tilde{\mathbb{T}}$ is isomorphic to $\mathbb{G}_m$ over $\mathbb{F}_\ell$.

(b) If ℓ is inert in K, then the composition of Ψ and reduction maps (mod ℓ) results in an embedding $\tilde{\Psi}_\ell : \tilde{\mathbb{T}}(\mathbb{F}_\ell) \hookrightarrow \mathbb{F}_{\ell^2}^\star$. Therefore, it suffices to note that $\tilde{\mathbb{T}}(\mathbb{F}_\ell)$ maps to elements of norm 1 in $\mathbb{F}_{\ell^2}$. ∎

LEMMA 1.2. *Let ℓ be a prime which splits in K with $\mathrm{ord}_\ell(y_0) = 0$. Let q be a rational prime. Then the following conditions are equivalent:*

(1) *$q \mid (\ell - 1)$ and $\bar{\alpha}^{(\ell-1)/q} = 1$ in $(\mathcal{O}_K/\wp\mathcal{O}_K)^\star$, where $\wp \mid \ell$ is a prime in $\mathcal{O}_K$.*

(2) *ℓ splits completely in $E_q/\mathbb{Q}$.*

(3) *$(\ell, E_q/\mathbb{Q}) = \mathrm{id}$.*

Proof. Since $\mathcal{O}_K/\wp\mathcal{O}_K \cong \mathbb{F}_\ell$, (1) $\Leftrightarrow q \mid \ell - 1$ and $x^q \equiv \alpha \bmod \wp$ has a solution in $\mathcal{O}_K$. Hence (1) is equivalent (2) as well as (3). ∎

We set

$$M_\alpha^+ = \{\ell \in \mathbb{P} : \ell \text{ splits in } K \text{ and the order of } \alpha \text{ modulo } \ell \text{ is } \ell - 1\},$$

$$M_\alpha^- = \{\ell \in \mathbb{P} : \ell \text{ is inert in } K \text{ and the order of } \alpha \text{ modulo } \ell \text{ is } \ell + 1\}.$$

Then $M_\alpha = M_\alpha^+ \cup M_\alpha^-$ and we have the following

COROLLARY 1.3. *Let ℓ be a prime which splits in K with $\mathrm{ord}_\ell(y_0) = 0$. Then $\ell \in M_\alpha^+$ if and only if $(\ell, E_q/\mathbb{Q}) \neq \mathrm{id}$ for any prime q.*

To study M_α^- we start with

LEMMA 1.4. *Let ℓ be an odd prime which is inert in K with $\mathrm{ord}_\ell(y_0)=0$.*

(a) *Let q be an odd prime. Then the following conditions are equivalent:*

(1) $q \mid (\ell+1)$ *and* $\bar{\alpha}^{(\ell+1)/q}=1$ *in* $(\mathcal{O}_K/\ell\mathcal{O}_K)^\star$.

(2) $q \mid (\ell+1)$ *and ℓ splits completely in* E_q/K.

(3) $(\ell, E_q/\mathbb{Q}) \subseteq C_q^-$.

(b) *The following conditions are equivalent:*

(1) $\bar{\alpha}^{(\ell+1)/2}=1$ *in* $(\mathcal{O}_K/\ell\mathcal{O}_K)^\star$.

(2) *ℓ splits completely in* $K'/\mathbb{Q}$.

(3) $(\ell, E_2/\mathbb{Q}) \subseteq C_2^-$.

Proof. Let γ be an element in $\mathcal{O}_K$ satisfying $\langle\bar{\gamma}\rangle=(\mathcal{O}_K/\ell\mathcal{O}_K)^\star$. Since $\bar{\alpha}^{\ell+1}=1$, one has that $\bar{\alpha}=\bar{\gamma}^{(\ell-1)t}$ for some integer t.

(a) It is easy to see that

$$(1) \Leftrightarrow q \mid \ell+1 \qquad \text{and} \qquad x^q \equiv \alpha \bmod \ell \text{ has a solution} \Leftrightarrow (2).$$

Recall that ℓ is inert in K if and only if $(\ell, K/\mathbb{Q})=\sigma_0$ and also that $q \mid (\ell+1)$ if and only if $(\ell, \mathbb{Q}(\boldsymbol{\mu}_q)/\mathbb{Q})=\tau$. We have (2) $\Leftrightarrow$ (3), because that ℓ splits completely in E_q/K is equivalent to $\sigma^2=\mathrm{id}$ for all $\sigma \in (\ell, E_q/\mathbb{Q})$.

(b) Since $\mathrm{ord}_\ell(y_0)=0$, $\bar{\alpha} \notin \mathbb{F}_\ell$ and $\sqrt{\bar{\alpha}}=\bar{\gamma}^{(\ell-1)t/2} \in \mathbb{F}_{\ell^2}-\mathbb{F}_\ell$. We have

$$\begin{aligned}(1) &\Leftrightarrow t \text{ is even} \Leftrightarrow \sqrt{\bar{\alpha}}^{\ell+1}=1\\ &\Leftrightarrow \left(\sqrt{\bar{\alpha}}+\frac{1}{\sqrt{\bar{\alpha}}}\right)^\ell=\sqrt{\bar{\alpha}}+\frac{1}{\sqrt{\bar{\alpha}}}\\ &\Leftrightarrow \sqrt{\bar{\alpha}}+\frac{1}{\sqrt{\bar{\alpha}}} \in \mathbb{F}_\ell \Leftrightarrow (2).\end{aligned}$$

From the definition of C_2^-, it is clear that (2) $\Leftrightarrow$ (3). ∎

COROLLARY 1.5. *Let ℓ be an odd prime which is inert in K with $\mathrm{ord}_\ell(y_0)=0$. Then $\ell \in M_\alpha^-$ if and only if $(\ell, E_q/\mathbb{Q}) \notin C_q^-$ for any prime q.*

Let s be the largest positive integer such that $\alpha \in (K^\star)^s$ and for any positive integer n, let $n_1=n/\gcd(s,n)$. The following Lemma gives a formula for d_n.

LEMMA 1.6. *For a square-free positive integer n, let $k_n = K$ (resp. $K(\sqrt{\alpha})$) if $2 \nmid n$ (resp. $2 \mid n$), we have*

$$d_n = \begin{cases} \dfrac{2n_1\phi(n)}{3[k_n \cap \mathbb{Q}(\mu_n) : \mathbb{Q}]} & \text{if} \quad K = \mathbb{Q}(\sqrt{-3}),\ 3 \mid n \text{ and } \alpha \in (K(\mu_n)^\star)^3, \\ \dfrac{2n_1\phi(n)}{[k_n \cap \mathbb{Q}(\mu_n) : \mathbb{Q}]} & \text{otherwise.} \end{cases}$$

Proof. Our argument is based on the following:

SUBLEMMA. *Let F be a field, K_1 a finite abelian extension of F, and K_2 be a finite extension of F which is not Galois but with prime extension degree. Then K_1, K_2 are linearly disjoint over F and $[K_1K_2 : K_1] = [K_2 : F]$.*

For an odd prime q with $q \mid n$, let $E_{n,q} = k_n(\mu_n, \sqrt[q]{\alpha})$. Note that $k_n(\mu_n)$ is abelian over K and that $K(\sqrt[q]{\alpha})$ is not Galois over K except when $K = \mathbb{Q}(\sqrt{-3})$ with $q = 3$. Also one has that $[K(\sqrt[q]{\alpha}) : K] = 1$ or q depending on whether $\alpha \in (K^\star)^q$. By the Sublemma, we have $[E_{n,q} : k_n(\mu_n)] = q/\gcd(s, q)$ except when $K = \mathbb{Q}(\sqrt{-3})$ with $q = 3$. If $K = \mathbb{Q}(\sqrt{-3})$ and $3 \mid n$, then

$$[E_{n,3} : k_n(\mu_n)] = \begin{cases} 1 & \text{if} \quad \alpha \in (K(\mu_n)^\star)^3, \\ 3 & \text{if} \quad \alpha \notin (K(\mu_n)^\star)^3. \end{cases}$$

(Note that $\alpha \in (K(\mu_n)^\star)^3$ is equivalent to $\alpha \in (k_n(\mu_n)^\star)^3$.) Thus the $E_{n,q}$'s are linearly disjoint over $k_n(\mu_n)$ and we have

$$[E_n : k_n(\mu_n)] = \begin{cases} n_1'/3 & \text{if} \quad K = \mathbb{Q}(\sqrt{-3}),\ 3 \mid n, \text{ and } \alpha \in (K(\mu_n)^\star)^3, \\ n_1' & \text{otherwise,} \end{cases}$$

where $n' = n/\gcd(2, n)$ (then $n_1' = n'/\gcd(s, n')$). Therefore,

$$\begin{aligned} [E_n : \mathbb{Q}] &= [E_n : k_n(\mu_n)][k_n(\mu_n) : \mathbb{Q}] \\ &= [E_n : k_n(\mu_n)][k_n : \mathbb{Q}][\mathbb{Q}(\mu_n) : \mathbb{Q}]/[k_n \cap \mathbb{Q}(\mu_n) : \mathbb{Q}] \\ &= \begin{cases} \dfrac{2n_1\phi(n)}{3[k_n \cap \mathbb{Q}(\mu_n) : \mathbb{Q}]} & \text{if } K = \mathbb{Q}(\sqrt{-3}),\ 3 \mid n, \text{ and } \alpha \in (K(\mu_n)^\star)^3, \\ \dfrac{2n_1\phi(n)}{[k_n \cap \mathbb{Q}(\mu_n) : \mathbb{Q}]} & \text{otherwise.} \end{cases} \end{aligned}$$

∎

LEMMA 1.7. (a) *Suppose that s is* odd. *For a square-free positive integer n, we have*

$$c_n^- = \begin{cases} 0 & \text{if } K \text{ is real with } K \subseteq \mathbb{Q}(\boldsymbol{\mu}_n), \\ & \text{or if } K' \text{ is imaginary with } K' \subseteq \mathbb{Q}(\boldsymbol{\mu}_n) \text{ and } 2 \mid n, \\ & \text{or if } K'' \text{ is real with } K'' \subseteq \mathbb{Q}(\boldsymbol{\mu}_n) \text{ and } 2 \mid n, \\ 1 & \text{otherwise.} \end{cases}$$

(b) *Suppose that K is real and s is even. For a square-free positive integer n, we have*

$$c_n^- = \begin{cases} 0 & \text{if either } K \subseteq \mathbb{Q}(\boldsymbol{\mu}_n) \text{ or } 2 \mid n, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. (a) If K is real with $K \subseteq \mathbb{Q}(\boldsymbol{\mu}_n)$, it is clear that there exists no element in G_n satisfying both $\sigma|_K = \sigma_0$ and $\sigma|_{\mathbb{Q}(\boldsymbol{\mu}_n)} = \tau$. Therefore, $C_n^- = \varnothing$. Similarly, if either K' is imaginary with $K' \subseteq \mathbb{Q}(\boldsymbol{\mu}_n)$ and $2 \mid n$ or K'' is real with $K'' \subseteq \mathbb{Q}(\boldsymbol{\mu}_n)$ and $2 \mid n$, there exists no element in G_n satisfying $\sigma|_K = \sigma_0$, $\sigma|_{K'} = \mathrm{id}$ and $\sigma|_{\mathbb{Q}(\boldsymbol{\mu}_n)} = \tau$ and thus $C_n^- = \varnothing$.

Now, suppose that neither of the above holds. For a square-free positive integer n, let $n' = n/\gcd(2, n)$. Choose $\sigma \in G_n$ such that $\sigma|_K = \sigma_0$, $\sigma|_{\mathbb{Q}(\boldsymbol{\mu}_n)} = \tau$, and $\sigma|_{K'} = \mathrm{id}$, if $2 \mid n$. After modifying σ by an element of $Gal(E_n/k_n(\boldsymbol{\mu}_n))$ we may assume that $\sigma(\sqrt[n']{\alpha}) = 1/\sqrt[n']{\alpha}$. Note $C_n^- \subseteq Gal(E_n/k_n(\boldsymbol{\mu}_n))\,\sigma$. Let ζ_n be a fixed primitive nth root of unity. Recall that $Gal(E_n/k_n(\boldsymbol{\mu}_n))$ is isomorphic to $\mathbb{Z}/n_1'\mathbb{Z}$ and given an element $\rho \in Gal(E_n/k_n(\boldsymbol{\mu}_n))$, it corresponds to a unique integers $i \in \mathbb{Z}/n_1'\mathbb{Z}$ provided $\rho(\sqrt[n']{\alpha}) = \zeta_{n_1'}^i \sqrt[n']{\alpha}$. It is routine to check that $(\rho\sigma)^2 = \mathrm{id} \Leftrightarrow 2i = 0$. Therefore, $\rho\sigma \in C_n^-$ if and only if $i = 0$ and thus $c_n^- = 1$.

(b) Recall that $K = K'$. If $2 \mid n$, then there exists no element in G_n satisfying $\sigma|_K = \sigma_0$, $\sigma|_{K'} = \mathrm{id}$. Hence $C_n^- = \varnothing$. The rest of the proof is similar to (a). ∎

2. CALCULATION OF THE DENSITY

Given $K = \mathbb{Q}(\sqrt{m})$, and fixing $\alpha = x_0 + y_0\sqrt{m} \in K$ with $N_{\mathbb{Q}}^K \alpha = 1$ as in the previous section. Following the analytic argument of Hooley [3], cf. also Murty [5], it is not difficult to establish the existence of densities for the sets of primes M_α^+ and M_α^-. We just state the result here without proof.

THEOREM 2.1. *Assume GRH holds. Then both* $\mathrm{den}(M_\alpha^+)$ *and* $\mathrm{den}(M_\alpha^-)$ *exist and are given by* $\mathrm{den}(M_\alpha^+) = \sum_n (\mu(n)/d_n)$ *and* $\mathrm{den}(M_\alpha^-) = \sum_n (c_n^- \mu(n)/d_n)$.

In order to derive a more explicit formula for the densities, we define for a quadratic field F,

$$\chi(F) = \begin{cases} 1 & \text{if } F \text{ is real,} \\ -1 & \text{if } F \text{ is imaginary.} \end{cases}$$

For integers n and s, let

$$A_s = \prod_{q \mid s,\, q \neq 2} \left(1 - \frac{1}{(q-1)}\right) \prod_{q \nmid s \text{ or } q = 2} \left(1 - \frac{1}{q(q-1)}\right)$$
$$\left(= A \cdot \prod_{q \mid s,\, q \neq 2} \frac{q^2 - 2q}{q^2 - q - 1} \right)$$

and

$$\psi_s(n) = \mu(|n|) \prod_{q \mid n,\, q \mid s,\, q \neq 2} \frac{1}{q-2} \prod_{q \mid n,\, q \nmid s} \frac{1}{q^2 - q - 1}.$$

Note that $|\psi_s(n)| \leqslant 1$ always hold.

Let D_F denote the discriminant of quadratic field F. We have moreover that $|\psi_s(D_F)| \leqslant \frac{1}{5}$ for all F except

$$\psi_s(D_F) = \begin{cases} -1 & \text{if } F = \mathbb{Q}(\sqrt{-3}) \text{ and } 3 \mid s, \\ -\frac{1}{3} & \text{if } F = \mathbb{Q}(\sqrt{5}) \text{ and } 5 \mid s, \\ \frac{1}{3} & \text{if } F = \mathbb{Q}(\sqrt{-15}) \text{ and } 15 \mid s. \end{cases}$$

We are ready to derive an explicit density formula for the case $K \neq \mathbb{Q}(\sqrt{-3})$.

THEOREM 2.2. *Assume GRH holds and suppose $K \neq \mathbb{Q}(\sqrt{-3})$. Let s be the largest positive integer such that $\alpha \in (K^\star)^s$. We have*

(a) *If s is* odd, *then the density of M_α is given by*

$$\operatorname{den}(M_\alpha) = A_s \left(1 + \frac{1-\chi(K)}{2}\psi_s(D_K) - \frac{1+\chi(K')}{2}\psi_s(D_{K'}) - \frac{1-\chi(K'')}{2}\psi_s(D_{K''})\right) > 0.$$

(b) *If K is real and s is even such that $N_{\mathbb{Q}}^K(\sqrt{\alpha}) = -1$, then the density of M_α is given by* $\operatorname{den}(M_\alpha) = A_s(1 - \psi_s(D_K)) > 0$.

Proof. We first determine the field K' explicitly. Suppose that $\alpha = (a+b\sqrt{m})/d$, $a, b \in \mathbb{Z}$, $d \in \mathbb{Z}^+$ with $\gcd(a, b, d) = 1$. One can write $a+d = 2^i m_1 b_1^2$, $a-d = 2^i m_2 b_2^2$, with $m = m_1 m_2$, $b = 2^i b_1 b_2$ and $(\sqrt{\alpha}+1/\sqrt{\alpha})^2 = 2(a+d)/d$, where $i = 0$(resp. $i = 1$) if $a \not\equiv d \bmod 2$ (resp. $a \equiv d \bmod 2$). Then it is easy to see that $K' = \mathbb{Q}(\sqrt{2^{1-i} d m_1})$ and $K'' = \mathbb{Q}(\sqrt{2^{1-i} d m_2})$. Let m', m'' be the square-free integers so that $K' = \mathbb{Q}(\sqrt{m'})$, $K'' = \mathbb{Q}(\sqrt{m''})$, respectively. Note that $\gcd(d, m) = 1$ and also that $m < 0$ implies $m' > 0$. We set $m_0 = \operatorname{lcm}(m, m', m'')$.

(a) Suppose that s is odd. We will only write the case when $D_K \equiv D_{K'} \equiv D_{K''} \equiv 1 \pmod 4$, and in other cases the proofs are similar.

Let $n_1 = n/\gcd(s, n)$. To compute $\operatorname{den}(M_\alpha)$ in this case, we evaluate sums S_1, S_2:

$$S_1 = \sum_{2\nmid n,\, m\nmid n} \frac{2\mu(n)}{2n_1\phi(n)} + \sum_{2\nmid n,\, m\mid n} \frac{\left(1+\frac{(1-\chi(K))}{2}\right)\mu(n)}{n_1\phi(n)}$$

$$= \sum_{2\nmid n} \frac{\mu(n)}{n_1\phi(n)} + \frac{1-\chi(K)}{2} \sum_{2\nmid n,\, m\mid n} \frac{\mu(n)}{n_1\phi(n)}.$$

$$S_2 = \sum_{2\mid n,\, m\nmid n,\, m'\nmid n,\, m''\nmid n} \frac{2\mu(n)}{2n_1\phi(n)} + \sum_{2m\mid n,\, m_0\nmid n} \frac{\left(1+\frac{(1-\chi(K))}{2}\right)\mu(n)}{n_1\phi(n)}$$

$$+ \sum_{2m'\mid n,\, m_0\nmid n} \frac{\left(1+\frac{(1+\chi(K'))}{2}\right)\mu(n)}{n_1\phi(n)} + \sum_{2m''\mid n,\, m_0\nmid n} \frac{\left(1+\frac{(1-\chi(K''))}{2}\right)\mu(n)}{n_1\phi(n)}$$

$$+ \sum_{2m_0\mid n} \frac{2\left(1+\frac{(1-\chi(K))(1+\chi(K'))}{4}\right)\mu(n)}{n_1\phi(n)}$$

$$= \sum_{2\mid n} \frac{\mu(n)}{n_1\phi(n)} + \frac{1-\chi(K)}{2} \sum_{2m\mid n} \frac{\mu(n)}{n_1\phi(n)} + \frac{1+\chi(K')}{2} \sum_{2m'\mid n} \frac{\mu(n)}{n_1\phi(n)}$$

$$+ \frac{1-\chi(K'')}{2} \sum_{2m''\mid n} \frac{\mu(n)}{n_1\phi(n)}. \qquad \text{(Note that } \chi(K'') = \chi(K)\,\chi(K').\text{)}$$

Applying Lemma 1.6, Lemma 1.7, and Theorem 2.1, we have

$$\operatorname{den}(M_\alpha) = S_1 + S_2$$

$$= A_s\left(1 + \frac{1-\chi(K)}{2}\psi_s(m) - \frac{1+\chi(K')}{2}\psi_s(m') - \frac{1-\chi(K'')}{2}\psi_s(m'')\right).$$

For the positivity of the density, note that $\frac{1-\chi(K)}{2}\psi_s(D_K) \geqslant -\frac{1}{5}$, $-\frac{1+\chi(K')}{2}\psi_s(D_{K'}) \geqslant -\frac{1}{5}$, and $-\frac{1-\chi(K'')}{2}\psi_s(D_{K''}) \geqslant -\frac{1}{3}$. Therefore,

$$\operatorname{den}(M_\alpha) \geqslant A_s(1-\tfrac{1}{5}-\tfrac{1}{5}-\tfrac{1}{3}) > 0.$$

(b) Suppose that K is real and s is even with $N_{\mathbb{Q}}^K(\sqrt{\alpha}) = -1$. Recall that $K' = K$, $K'' = \mathbb{Q}$, and $c_n^- = 0$ if $2 \mid n$. We will only prove the case when $D_{K'} \equiv D_{K''} \equiv 1 \pmod 4$, since the case when $D_{K'} \equiv D_{K''} \not\equiv 1 \pmod 4$ can be proved similarly. We have

$$\begin{aligned}
\operatorname{den}(M_\alpha) &= S_1 + \sum_{2\mid n,\, m\nmid n} \frac{\mu(n)}{2n_1\phi(n)} + \sum_{2m\mid n} \frac{\mu(n)}{n_1\phi(n)} \\
&= \sum_{2\nmid n} \frac{\mu(n)}{n_1\phi(n)} - \frac{1}{2} \sum_{2\nmid n,\, m\nmid n} \frac{\mu(n)}{n_1\phi(n)} - \sum_{2\nmid n,\, m\mid n} \frac{\mu(n)}{n_1\phi(n)} \\
&= \frac{1}{2} \sum_{2\nmid n} \frac{\mu(n)}{n_1\phi(n)} - \frac{1}{2} \sum_{2\nmid n,\, m\mid n} \frac{\mu(n)}{n_1\phi(n)} \\
&= A_s(1-\psi_s(m)).
\end{aligned}$$

For the positivity, observe that $|\psi_s(D_K)| \leqslant \frac{1}{3}$, because $K \neq \mathbb{Q}(\sqrt{-3})$. Therefore, $\operatorname{den}(M) = A_s(1-\psi_s(D_K)) \geqslant A_s(1-\frac{1}{3}) > 0$. ∎

EXAMPLE. Consider $K = \mathbb{Q}(\sqrt{21})$ and $\varepsilon = (5+\sqrt{21})/2$, which is the fundamental unit in K. If we consider $\alpha = \varepsilon$, then $K' = \mathbb{Q}(\sqrt{7})$, $K'' = \mathbb{Q}(\sqrt{3})$, and according to Theorem 2.2, $M_\varepsilon = A(1-\psi_1(D_{K'})) = A$. Similarly, if we consider $\alpha = -\varepsilon$, then $K' = \mathbb{Q}(\sqrt{-3})$, $K'' = \mathbb{Q}(\sqrt{-7})$, and $M_{-\varepsilon} = A(1-\psi_1(D_{K''})) = \frac{42}{41}A$.

Remark 2.3. If K is imaginary and s is odd, then K'(resp. K'') is real(resp. imaginary) and $\operatorname{den}(M_\alpha) = A_s(1+\psi_s(D_K)-\psi_s(D_{K'})-\psi_s(D_{K''}))$.

For the case $K = \mathbb{Q}(\sqrt{-3})$, let D_3 be the least positive integer n such that $K(\sqrt[3]{\alpha}) \subset K(\boldsymbol{\mu}_n)$. Call it cubic conductor of α in K. Recall $\alpha = \beta^{\sigma_0}/\beta$ for some $\beta \in \mathcal{O}_K$. May assume that $\gcd(\beta, \beta^{\sigma_0}) = 1$. Since $\mathcal{O}_K$ is an unique factorization domain, can write $\beta = \pm\zeta_3^j \prod_{i=1}^t \pi_i^{a_i}$, where $j \in \{0, 1, 2\}$ (uniquely determined by α), $t \in \mathbb{Z}^+$, $a_i \in \mathbb{Z}^+$, for every $i \in \{1, 2, \ldots, t\}$, and π_i's are distinct primary primes in K. From the classical theory of cubic Gauss sums (cf. [4, Chap. 9]), one knows that $\pi_i^{\sigma_0}/\pi_i \in (K(\boldsymbol{\mu}_{p_i}))^3$, where $p_i = N_{\mathbb{Q}}^K \pi_i$. Then $\alpha/\zeta_3^j \in (K(\boldsymbol{\mu}_{p_1 p_2 \cdots p_t}))^3$ and it is easy to check the following

PROPOSITION 2.4.

(a) *If* $j=0$, *then* $D_3 \mid p_1 p_2 \cdots p_t$.

(b) *If* $j=1$ *or* 2, *then* $9 \mid D_3 \mid 9p_1 p_2 \cdots p_t$.

(c) *Write* $\alpha=(a+b\sqrt{-3})/d$, $a, b \in \mathbb{Z}$, $d \in \mathbb{Z}^+$, *with* $\gcd(a, b, d)=1$. *Then* $D_3 \mid 9d$.

If $K=\mathbb{Q}(\sqrt{-3})$ and $\gcd(6, s)>1$, where s is the largest positive integer such that $\alpha \in (K^\star)^s$, then it is easy to see that $\operatorname{den}(M_\alpha)=0$. We have finally (note that $1+\psi_s(3)=\frac{4}{5}$, if $3 \nmid s$) :

THEOREM 2.5. *Let* $d_0=\gcd(D_{K'}, D_{K''})$. *Assume GRH holds and suppose* $K=\mathbb{Q}(\sqrt{-3})$. *Suppose further that* $\gcd(6, s)=1$. *Then the density of* M_α *is given by*

$$\operatorname{den}(M_\alpha)=\tfrac{4}{5} A_s(1-\psi_s(d_0)-\psi_s(D_3)+\psi_s(\operatorname{lcm}(d_0, D_3)))>0.$$

Proof. If $9 \mid D_3$, then $\psi(D_3)=\psi(\operatorname{lcm}(d_0, D_3))=0$. The calculation of the density of M_α is exactly the same as in Theorem 2.2, because $\alpha \notin (K(\mu_n)^\star)^3$ for all square free integer n. Since K is imaginary, according to Remark 2.3, we have

$$\begin{aligned}\operatorname{den}(M_\alpha) &= A_s(1+\psi_s(3)-\psi_s(d_0)-\psi_s(3d_0)) \\ &= \tfrac{4}{5} A_s(1-\psi_s(d_0)) \geqslant A_s(1-\tfrac{1}{3})>0.\end{aligned}$$

(Note that $d_0=D_{K'}$ or $-D_{K''}$, $3 \nmid d_0$, and thus $-\psi_s(d_0) \geqslant -\frac{1}{3}$.)

Now suppose that $9 \nmid D_3$. Then D_3 is square free. Note that K'(resp. K'') is real(resp. imaginary) and thus $c_n^-=1$ for any square-free positive integer n. Also note that $D_{K'} \equiv D_{K''} \pmod 4$, because $D_K \equiv 1 \pmod 4$.

We will only prove the case when $D_{K'} \equiv D_{K''} \equiv 1 \pmod 4$, and the proof in the case when $D_{K'} \equiv D_{K''} \not\equiv 1 \pmod 4$ is similar.

Again we first compute two sums S_1, S_2 (note that $\gcd(6, d_0)=\gcd(6, D_3)=1$):

$$\begin{aligned}S_1 &= \sum_{2\nmid n,\, 3\nmid n} \frac{2\mu(n)}{2n_1\phi(n)}+\sum_{2\nmid n,\, 3\mid n,\, D_3\nmid n} \frac{2\mu(n)}{n_1\phi(n)}+\sum_{2\nmid n,\, 3D_3\mid n} \frac{3\cdot 2\mu(n)}{n_1\phi(n)} \\ &= \sum_{2\nmid n} \frac{\mu(n)}{n_1\phi(n)}+\sum_{2\nmid n,\, 3\mid n} \frac{\mu(n)}{n_1\phi(n)}+4\sum_{2\nmid n,\, 3D_3\mid n} \frac{\mu(n)}{n_1\phi(n)}.\end{aligned}$$

$$\begin{aligned}S_2 &= \sum_{2\mid n,\, 3\nmid n,\, d_0\nmid n} \frac{2\mu(n)}{2n_1\phi(n)}+\sum_{2\mid n,\, 3\nmid n,\, d_0\mid n} \frac{2\mu(n)}{n_1\phi(n)}+\sum_{6\mid n,\, d_0\nmid n,\, D_3\nmid n} \frac{2\mu(n)}{n_1\phi(n)} \\ &\quad+\sum_{6\mid n,\, d_0\nmid n,\, D_3\mid n} \frac{6\mu(n)}{n_1\phi(n)}+\sum_{6d_0\mid n,\, D_3\nmid n} \frac{4\mu(n)}{n_1\phi(n)}+\sum_{6d_0\mid n,\, D_3\mid n} \frac{12\mu(n)}{n_1\phi(n)}\end{aligned}$$

$$= \sum_{2 \mid n} \frac{\mu(n)}{n_1 \phi(n)} + \sum_{6 \mid n} \frac{\mu(n)}{n_1 \phi(n)} + \sum_{2d_0 \mid n} \frac{\mu(n)}{n_1 \phi(n)} + \sum_{6d_0 \mid n} \frac{\mu(n)}{n_1 \phi(n)}$$

$$+ 4 \sum_{6D_3 \mid n} \frac{\mu(n)}{n_1 \phi(n)} + 4 \sum_{6d_0 \mid n,\, D_3 \mid n} \frac{\mu(n)}{n_1 \phi(n)}.$$

Applying Lemma 1.6, Lemma 1.7, and Theorem 2.1, we have

$$\begin{aligned}
\operatorname{den}(M_\alpha) &= S_1 + S_2 \\
&= \sum_{n} \frac{\mu(n)}{n_1 \phi(n)} + \sum_{3 \mid n} \frac{\mu(n)}{n_1 \phi(n)} + \sum_{2d_0 \mid n} \frac{\mu(n)}{n_1 \phi(n)} + \sum_{6d_0 \mid n} \frac{\mu(n)}{n_1 \phi(n)} \\
&\quad + 4 \sum_{3D_3 \mid n} \frac{\mu(n)}{n_1 \phi(n)} + 4 \sum_{6d_0 \mid n,\, D_3 \mid n} \frac{\mu(n)}{n_1 \phi(n)} \\
&= A_s(1 + \psi_s(3) + \psi_s(2d_0) + \psi_s(6d_0) + 4\psi_s(3D_3) + 4\psi_s(6 \operatorname{lcm}(d_0, D_3))) \\
&= \frac{4}{5} A_s(1 - \psi_s(d_0) - \psi_s(D_3) + \psi_s(\operatorname{lcm}(d_0, D_3))).
\end{aligned}$$

For the positivity of the density, recall that $-\psi_s(d_0) \geqslant -\frac{1}{5}$ and note that $|\psi_s(D_3)| \leqslant \frac{1}{3}$, $|\psi_s(\operatorname{lcm}(d_0, D_3))| \leqslant \frac{1}{3}$, because $D_3 \geqslant 5$. Therefore, $\operatorname{den}(M_\alpha) \geqslant (1 - \frac{1}{5} - \frac{1}{3} - \frac{1}{3}) > 0$. ∎

REFERENCES

1. Y.-M. J. Chen, Y. Kitaoka, and J. Yu, Distribution of units of real quadratic number fields, *Nagoya Math. J.* **158** (2000), 167–184.
2. Y.-M. J. Chen and J. Yu, On a density problem for elliptic curves over finite fields, *Asian J. Math.* **4**, No. 4 (2000), 737–756.
3. C. Hooley, On Artin's conjecture, *J. Reine Angew. Math.* **225** (1967), 209–220.
4. K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," 2nd ed., Springer-Verlag, New York, 1990.
5. M. R. Murty, On Artin's conjecture, *J. Number Theory* **16** (1983), 147–168.
6. H. Roskam, A quadratic analogue of Artin's conjecture on primitive roots, *J. Number Theory* **81** (2000), 93–109; Erratum, **85** (2000), 108.